00:00
Speaker 1
You.

00:03
Speaker 2
Hello and welcome to the Human and Machine podcast. My name is Jaco. I am your co host. As always, here with my co host, Lenny Smith. Lenny, welcome back.

00:12
Speaker 3
Thanks, Jaco. It's quite a miserable day outside. It's quite a rainy day here in Jobik today, but be glad to be back to shoot another podcast. Can't believe it's episode number 1717.

00:22
Speaker 2
Podcast number 17 has been phenomenal to everybody listening. Thank you so much for your support, suggestions, and just topics and conversations we've been having. Thank you for listening and thank you for spreading the word. We appreciate the support. We are, of course, the Human and Machine podcast, talking about everything in the industrial, manufacturing, landscape, technology. Best practice topic for today is a fascinating one we should have covered a long time ago already is the topic of cybersecurity. And we're quite fortunate this week to be chatting with Brian Pinnock. Brian is a senior director of sales engineering at Mimecast, big global cybersecurity business.

01:04
Speaker 2
And Lenny, I think everything we've spoken about over the past couple of weeks and episodes on IoT, Industry 4.0, convergence of it and OT, all of these topics, I think one of the underlying themes that not only in the podcast, but also through discussions, as day to day discussions has been coming out, is the topic of cybersecurity. No, definitely.

01:25
Speaker 3
I think we've been talking IoT, well, industrial IoT, quite a lot in a lot of our podcast series. Analysts predict that by 2025, we would have 21.5 billion IoT devices connected.

01:41
Speaker 2
It's crazy.

01:42
Speaker 3
That's insane. And if we haven't had enough three letter acronyms in this industry, we're going to definitely learn a lot on them today as well. But the problem that we're seeing is that these devices that bridge kind of the IoT, the OT, and the IT gap, they are considered to be CPS systems. Now, CPS is considered a cyber physical.

02:07
Speaker 2
System, and that's edge. More edge types, more edge types.

02:11
Speaker 3
And the reason why they see that for edge devices is because they are the device that bridge both the digital world, obviously the connection to the cloud, but also have that connection to the physical world because they connect to the physical devices. And they say that these CPS devices are great adversaries, obviously, for people to try hacks and connect. So, yeah, it is something that is really going to be targeted when we go forward into this.

02:40

Speaker 2
Well, we think it is what they say. We're not the experts. That's why we have Brian there. And I think everything we've spoken about industry 4.0 and the proliferation of devices and IoT and edge is, what are those threat. What does the threat landscape look like? Where do we see the threats coming from? So, Brian, it was a very long intro. Sorry, we tend to do this sometimes, but welcome to the Human and Machine podcast. It's really cool to be chatting to you today.

03:07
Speaker 1
Thank you very much.

03:08
Speaker 2
So I suppose before we get into what the landscape looks like and what is happening, and I'm sure you see some really scary stuff in your role and what you guys do every day, you see some really scary stuff. You've been in this industry for a while.

03:25
Speaker 1
Yeah, no, I have. Maybe just to give you a little bit of my background, I kind of finished university in the early 1990s, and I guess cybersecurity back then was relatively straightforward. And the reason I'm sort of mentioning it is there was just about the time of the advent of the Internet, and we started learning some very hard lessons in the cybersecurity side of things. So it started out with the initial attacks came at the endpoints with viruses, and we had all kinds of interesting viruses back in those days, and they were relatively easy to stop because networks weren't that pervasive yet, and they were quite segmented. But as the Internet grew and everything started to connect together, these viruses just found a way to spread dramatically. I guess the current Covid-19 thing is a great analogy for that.

04:09
Speaker 1
But at the end of the day, people were still focused on protecting their perimeter because networks were very much centered around the data center and the kind of head office and that sort of thing, and then the endpoints, and it didn't get much more sophisticated than that. And if you want to use that as analogy for IoT today, that's kind of where things are. It's almost like we've thrown out all of those security learnings that we got in the early 1990s, hardwind learnings, and we're kind of starting back from scratch again with that kind of in the mid, early to mid two thousand s. I wasn't that focused on cybersecurity side of things. I was more in network based kind of industries. I worked for companies like Dimension data. We actually started my own company for a while that did systems integration type work.

04:54
Speaker 1
Again, very network focused, and then moved into a research and development type position at a company called Internet Solutions, which has now been folded into dimension data. And that started getting me back into cybersecurity. And in fact, it was quite amazing how much things have changed. And we can maybe talk a little bit about why things are so different now than they were kind of earlier on. What has actually fundamentally changed. I then moved into mimecast in 2016, and that really sort of kind of reimmersed me in the whole security landscape side of things.

05:26
Speaker 2
Very much at the forefront.

05:28
Speaker 1
Yeah, absolutely. I mean, emailed is kind of the number one attack vector still, and that is probably the sort of core of what mimecast does. Obviously, we do web security and a number of other things as well, which we can chat about as far as it kind of impacts cybersecurity as a whole. But that's been sort of a huge, steep learning curve for me as to just how much things had changed and moved on and how much more severe things have actually got than they were, say, even as short time ago as kind of 2012, there's been a dramatic change.

05:57
Speaker 2
Yeah, it's fascinating. We were chatting beforehand. We were saying, in our world and the manufacturing and the OT world specifically, cybersecurity was something that was very much placed on the map when we first heard about the stuxnet virus affecting all the, I think at that time, what was focused on Siemens control systems, focusing key infrastructure and water and wastewater, and that's when it became very prevalent. But it's very interesting what you said, and maybe this is a massive unknown to people, is that email, even though we speak about edge intrusion and edge and devices and the threats presented in that world, it's fascinating how email is the number one attack vector. That's absolutely fascinating. And I think certainly our listeners and people in our industry don't know that.

06:44
Speaker 1
I think particularly people who not too focused on the whole cybersecurity picture, often a sort of naive view is, well, my email is not that important to me. I can actually live without my email. So I don't really need to defend and protect my email as much as maybe I need to defend and protect my operational support systems and business support systems. And the reality is, we're not saying, look, there is obviously a degree email is a lot more important than people realize, but that's a separate issue. But it's the initial entry points, the initial foothold that cyber attackers use to get into organizations. And then from there, they spread laterally and start impacting different types of systems, whether they're business systems or production systems.

07:22
Speaker 1
And that's what people don't realize is if you had to design the perfect system to get into just about every company in the world, sort of a backdoor in, that was very hard to close. You'd probably design something that looked a lot like email, and that's becoming a challenge.

07:38
Speaker 2
Yeah, I'm thinking about the communication. I mean, that we typically see, let's call it the information value chain that we have in your typical manufacturing business. It's fascinating that all of that, outside of threats, perhaps. It's still fascinating that a lot of the comms internally, and these are mission critical comms in terms of how departments communicate around with each other, around production data, around alerts that happen, is all email based. And the ability for a system to actually interact with people via email, that presents a much bigger threat to these manufacturing companies. If email is the primary way that communication happens, not only between people, but also machines and people.

08:24
Speaker 1
Yeah, we actually find that quite often, it doesn't matter how sophisticated an organization is, they might have a very highly digitized enterprise resource planning system and a very. What's the word I'm looking for? Sort of formalized type data system. And structured data is the kind of words, and they're quite good at protecting that. But often you find there's elements of that which are part of the critical path of either manufacturing something or getting it to market. So we've seen organizations where the manufacturing side was absolutely fine, but they used email as a kind of informal workflow system for their logistics. So it didn't matter that they could manufacture everything, they just couldn't get it out of the. From the production facilities to the warehouse facilities and beyond because the email was down. So you see that sort of thing.

09:07
Speaker 1
It is very much what we call your unstructured data. And it's one of the hardest things to, first of all, protect, and then second of all, to kind of manage and make sure that you don't have things like data leaks and things, because there's a lot of corporate intellectual property that is kept in things like email, things like word documents, things like PowerPoint slides, that's kind of all sitting in email. It's like the corporate memory almost, in a way.

09:30
Speaker 2
Yeah, 100%. And for manufacturing, I mean, if we think about who would know the reasons why, I would

imagine that very often, more than often, it's monetary. But if we look at in the manufacturing world, I don't know, you would need to tell us in terms of some of the objectives or motives behind these attacks. I think the one that you've just mentioned now is very important, is about intellectual property, competitive advantage that exists within a business. That would typically be the objective to get that ransomware holding operations and data hostage. Is that what you find some of the motives behind these attacks and intrusions?

10:12
Speaker 1
Yeah. So I think what you first got to understand, and this is also something if you're not sort of really up to date with what's happening in the cybersecurity landscape, and the media, unfortunately, is not our friend in this space. They always put that picture of that sort of hacker with a hoodie and often little ones and zeros floating around them. And that's not what your typical cyber threat actor actually looks like anymore. What you actually have are highly sophisticated networks. They're run as a business and they can take on various forms. So sometimes they are nation state or nation state sponsored actors, and that can be quite important. If you are part of critical infrastructure of some kind. Often they target that for putting sleep of malware into your systems so that they can maybe take down production facilities at a later date.

11:04
Speaker 1
So there's a whole bunch of reasons that your state sponsored actors might be interested industrial sort of side of.

11:13
Speaker 2
Things, especially with critical infrastructure like water, wastewater treatment plants, power generation plants. And these are obviously some of the folks that we deal with on a daily basis, and that's obviously a massive concern for them.

11:26
Speaker 1
Absolutely, yeah. And in fact, what's interesting is the sort of definition of critical infrastructure has actually got a lot broader quite recently. So organizations that may not necessarily have considered themselves critical infrastructure actually now part of critical infrastructure for exactly this reason. It serves a political purpose to potentially cause some degree of disruption. And it's quite interesting. If you wanted to create a weapon against a country, what you would want is something that's quite sophisticated that you could dial up or dial back. If you just throw a nuclear weapon at a dam or a power station or something, that's kind of very blunt instrument. Whereas if you just caused small disruptions, you could potentially cause instability in a political system somewhere. So there's a lot that nation state actors are interested in. More often than not, though, they're interested information.

12:14
Speaker 1
I mean, what we've seen in South Africa specifically is at mimecast, we don't do what we call thread attribution, and there's a whole bunch of reasons for that. I'll leave it to your imagination which types of countries would be interested in this sort of data, but quite often what they've got is they're actually just listening.

12:31
Speaker 2
Name it one hand.

12:34
Speaker 1
Yeah. And sometimes there are false flag efforts, but more often than not, where they smoke this fire and what it seems to be is exactly what it is, because often they're not even highly sophisticated because manufacturing typically is not that highly sophisticated when it comes to cyber protection. And I say that as compared to, for example, say, financial services, which is generally a lot more mature with a lot more sort of people involved. So what we've seen is a number of things. So you can actually split the types of attacks up into low sophistication, high volume, and that you could call kind of almost a spray and pray type attack.

13:11
Speaker 1

And really what they're doing, they're saying, if you're the kind of organization that is very weak on your cyber hygiene, you got a lot of holes, you've got a lot of unpatched systems, all of those kind of things. We're going to throw a whole bunch of stuff at you, and some of it might stick. And those are kind of fairly simple and relatively easy if you just do all the right things to block. Where it gets a little bit more challenging is when you have the low volume, high sophistication type attacks. And that would be someone who wants to get into your network. And so I'm taking a long time to get to the example. But for example, just watch production schedules. That kind of information is super valuable to certain individuals.

13:49
Speaker 1
And we've seen that before, where organizations found they did penetration testing and found that they'd actually been penetrated and then realized there was actually malware on their systems that was apparently doing nothing other than reporting back on what was going on with their ScaDA systems and things like that. And one is only making a supposition as to why would they want to do that as opposed to bringing it down. And it really is just to get a view of just what the kind of capacity and capability is of organ. And if you think about that in the sort of context of one production facility or one factory, whatever, probably not that meaningful. If you could get that across an entire country, there's a lot of very good information that you're getting.

14:31
Speaker 2
An entire industry relating to that country could be very valuable.

14:35
Speaker 1
Exactly. Yeah. The other things that we see are sometimes ransomware. I mean, that's a relatively simple thing. As I say, attackers typically are after two things. And it's normally, if they're just after information, the second order effect is they want to monetize that information in some way. And sometimes they're after actually dropping malware literally into your space. And ransomware is kind of the combination of those things. Because if I had to steal all your information, it's got to be valuable to someone so I can potentially sell it on the open market in some way, but the one organization that is the most valuable to is yourself.

15:08
Speaker 1
So if I have to block off all of your production systems or your business support systems, whatever they might be, and hold you to ransom, you're the one person who's going to actually pay me money, or the most likely person to actually pay me money to get that back. So ransomware is kind of almost an in place combination of those two things, control the information and then monetize it in place. But we see there's a whole bunch of ones, and maybe let's just talk about them in general, probably the next biggest one, which is not specific to sort of heavy or light industry, for that matter. It's across the board, but it's quite amazing how effective it is. There's something we call business email compromise, and that's where there's no actual malware or sort of malicious links or anything sent in.

15:50
Speaker 1
We literally just, if we're a threat actor, we send you or the appropriate person an email that purports to be. It's an impersonation email, pretends to be your CEO or your CFO, and has some kind of urgent message to say, please pay us. Know we've got a huge deal that's pending on you doing a deposit of some kind. And we've seen large organization airplane parts manufacturers in Austria. I think the biggest one, it was something like €50 million over the course of about six or seven different stages of this particular attack. And that comes back to the whole human error and people being, and I don't want to use the word gullible, but I think trusting, our natural state of mind is to be trusting, especially if you're dealing with someone you believe is someone inside your organization.

16:37
Speaker 1
Yes, those would be the big ones.

16:44
Speaker 3
There's actually examples of that. In 2019, we spoke about state sponsored attack. There was a state sponsored

attack, russian state sponsored attack. Trying to use fact. You said you can call them on your fingers, but it's fact. And exactly that. Brian, you also spoke about devices that could potentially become a hole or plug a hole in your security device. They used a VoIP phone. They tried a VoIP phone, office printer, even a network video recorder, and they found a way to get in and exactly that. These high volume attack, luckily not trying to steal information. They call it another acronym for us for today, a DDoS or a distributed denial of service attack.

17:33
Speaker 2
Yeah, we're not going to get into.

17:34
Speaker 3
That one, I think, but means you pretty much just overwhelm the computer system with traffic, and you pretty much commit there. But the point is 100% with this onslaught of IoT, and I think the ease of just plugging it in absolutely becomes a whole. And if you don't cater for that correctly, then yeah.

17:51
Speaker 2
And Brian, what we've seen on our side, at least the conversations that we have on a daily basis, is that over the last couple of years in the manufacturing world, what has been a little bit frustrating for the folks on our side, is that the two networks were very separate. So your manufacturing plant floor was on a specific network, and then the rest of your business was on another network. And the plant floor was always seen to be intrinsically, it was safe, it was separate, it was secure. But now, with all of these different digital transformation initiatives that most of the manufacturers are kicking off, there's a big drive to get all of that onto one network. And obviously with that, you've got the exposed risk and ease of use to get access to those systems and those machines.

18:36
Speaker 2
And obviously, on the back of that cybersecurity is now, all of a sudden, for these manufacturers, for most of them, just based on the conversations that we've had, something that they have to brush up their education on, the understanding they have to consider it a lot more than what they have in the past. And all of a sudden, it's a big topic for them. It and ot convergence. Sorry.

19:03
Speaker 1
If you go back in time a little bit, you can actually see why it's problematic. If you go back to the good old SCaDA systems, they tended not to be TCP IP, they tended to be these fairly arcane type protocols, typically serial rs four nine and rs two three two, and those sorts of things.

19:19
Speaker 2
But they were very, weren't built to be online.

19:22
Speaker 1
No, absolutely. The other problem that you've got with IoT type systems, and it's a universal problem, is in the old days, because of the cost of doing something, it was very expensive to have a multipurpose computer, but much cheaper to have something that was custom made to do one task. And if something's custom made to do one task, it's very hard to fool it into doing something else. What we're seeing now is this rise of very cheap multi purpose computers. The raspberry PI is the most famous, but there are literally hundreds of knockoffs of equivalent sorts of things. And the trouble with that, though, is you might have taken a multipurpose computer and you've loaded some software on it to make it do a specific task, but there's a whole bunch of open ports and capabilities built into that multipurpose computer.

20:07
Speaker 1
Now, that could be used for a number of other things, and they're effectively sort of security vulnerabilities that are just sort of waiting to be exploited. So it's much harder to defend against these.

20:18

Speaker 3
Exactly. And you installed the OS that you got five years ago, and you left it and you never updated the firmware. And the thing with the latest, the security patches that comes with.

20:27
Speaker 2
Because it's not priority.

20:28
Speaker 3
Because it's not priority. So 100%, we see a lot that an IoT device is left with the original firmware and nobody really updates those things anymore.

20:38
Speaker 2
And Brian, you're 100% correct. And I think why that a lot of that is happening is when we talk about these digital transformation projects, especially in our world of mining, manufacturing and infrastructure, scaling is a massive consideration in terms of cost. So all of a sudden, the standards, in terms of what is acceptable as far as hardware goes, drops significantly because it becomes purely a costing. And some of these sort of cheap and nasty kind of edge devices are okay because it helps us with scaling and reaching the kind of volume of connectivity that we need. And very often, the budget doesn't allow for that kind of scaling around the devices. So these cheaper nasties and everything that they will allow, potentially the risks that they present are okay.

21:22
Speaker 2
And people and these guys, these leaders in these industries, are okay with that because it fits the budget, it fits.

21:28
Speaker 1
The ball, and it's a challenge. I mean, you see it in healthcare with these sort of real time operating systems. And obviously healthcare, there's literally lives on the line. So it's much easier to kind of create standards and say that you may not do x and you may not do y. It's a little bit harder to do that in an industrial side of things. Obviously, there's health and safety aspects, and there are sometimes lives on the line depending on what systems you're talking about. But you can sometimes use these multipurpose operating systems that were never designed for real time use. And that also talks to the patching side of things. It's all very well in a corporate type environment. A head officer say you've got a patch and make sure that everything's up to date. And it is.

22:06
Speaker 1
A key aspect of cybersecurity is making sure you're always up to date. It's much harder to do that in, say, a 24/7 facility where you can't actually have downtime and you can't have run the risk of loading a patch that might block some vulnerability that may or may not be exploitable. And the risk that you face on that front is you might actually bring down your whole production facility because there's some unforeseen consequence of patching your system. So it does get a lot harder in the industrial space than it is, for example, in the sort of enterprise corporate space.

22:36
Speaker 2
Yeah. Brian, you mentioned something I just want to ask you about. So you mentioned human error. So in our world, obviously in a live kind of production environment, where safety is obviously a massive critical factor, especially at a mine, you can imagine human error is perhaps something a little bit different to your definition of human error. When you say human error, it sounds quite scary. What does that mean in terms of cybersecurity and awareness and maybe some observations around human error.

23:12
Speaker 1
So I actually like flipping that around and calling it the human firewall. So what you can do is there's no security system that's completely invulnerable. And I think that's the first thing everybody needs to realize, is any chief information security officer worth assault will tell that to the board when they get appointed. To say, my job here is not to stop you being breached. My job here is to work is to ensure that the consequences of that breach

are as limited as possible and the recovery from that breach is as quick as possible. And one of your biggest vulnerabilities is your people. And what you can do is you can turn that vulnerability or that weak point into a strength by creating a human firewall and trying to, you can never entirely eliminate, but try to reduce human error.

23:59
Speaker 1
And we've actually got some really good statistics. There's obviously a whole bunch of psychology that's involved here. So the first way we tried to do that in the cybersecurity industry was put people down in front of these long, boring, sort of cybersecurity sort of policies and procedures and awareness training type things. And we bored the life out of everyone. And then we wondered why nobody paid attention. So what's quite interesting, actually, Michael Madden, who started a company called Atata, who was ultimately bought up by mimecast, actually recognized this. He was in the treasury department, the US Treasury Department, and in the cybersecurity section of things.

24:33
Speaker 1
And he actually looked around while he was doing his mandatory cybersecurity training, and he looked at, these are all cybersecurity professionals, and what they'd done is they put their cybersecurity training video onto one screen and we're completely ignoring it, looking at something else, and literally just running the clock down on this video that they were all forced to watch. And he said, this system is completely broken. We need to do this another way.

24:54
Speaker 2
In other words, in no way measuring the actual effectiveness of the train.

24:58
Speaker 1
Not at all. It was literally a checkbox exercise.

25:00
Speaker 2
It was a tick box. Everybody was okay because they attended. And we're good, our posture is good, and our hygiene is good.

25:06
Speaker 1
Correct. And this applies probably to things like health and safety and all of these sorts of things where if you think you just send someone a video that they got to watch and you think they're watching it, they probably aren't. And even if they are watching it, they're not paying attention. And so he then did a whole bunch of research, and there's quite a lot of very good research data on this now. Is that what you got to do to make people actually engage with the content is keep it short, keep it engaging. Humor is a really good way to do that. Make it repeatable and make it meaningful in people's lives and make them part of the solution to the problem and just keep kind of cycling through that.

25:45
Speaker 1
And what's quite nice is we've actually been running for a couple of years now with a system, and we then did a sort of little bit of research on our own platform to say those of our clients who'd actually bought the mimecast awareness training, which kind of works on those principles where it's short, engaging users, humor, all of those kind of things, versus clients of ours who either had other awareness training systems or who had no awareness training systems. And we then looked at what their riskiness was for certain end, for different end users. And we found that users who had mimecast awareness training were five times less likely to be taken in by things like phishing attacks and clicking on bad links and all of those kinds of things. So the kind of numbers, the hard numbers are in now.

26:27
Speaker 1
And I think that's where I'm not saying you necessarily have to buy mimecast if you want to do that, but what

you need to do if you're trying to build your human firewall is you actually need to look past the vanity metrics of number of people who've watched videos, whatever. You've really got to look at engagement and ultimately look at are they actually doing bad things anymore? Are they not? And you got to find a way to make that measurable.

26:49
Speaker 2
Yeah, absolutely. The importance, the month of October was obviously cybersecurity Awareness month. And my immediate thoughts when I realized, or at least saw that it was cybersecurity month is, where did it start? Where does it come from? Why? A whole month dedicated to cybersecurity awareness. And that's when the topic of human error and the human firewall, as you call it, and the importance of us and our interactions every day and the decisions and choices we make, that's when it became quite obvious to me with the importance of cybersecurity awareness, that we, in fact, had a whole month dedicated to it. Globally. Had a whole month dedicated to it.

27:34
Speaker 1
Yeah. So it started actually in. I might have my date wrong, but it's in the early 2000s, about 2004, and it started in the US between the National Cybersecurity alliance and the US Department of Homeland Security, if I'm not mistaken. And it's quite interesting how that's grown over the years. It really kind of was below the radar for a very long time. And now it's actually taken on, first of all, national in America and then became international. And there's been a kind of a love hate relationship between the sort of business community in the US and the government, because the government, on the one hand, is trying to encourage the business community to be more cyber aware and to build better cybersecurity. There's actually a really good observation.

28:21
Speaker 1
In the Ukraine, when the notpetcha virus hit, it obviously took down a big chunk of the Ukraine, and it also then spread globally and became a kind of global pandemic. And there were some very big manufacturing organizations that were hit, and logistics companies. There was Mersk, there was TNT, which is part of FedEx. There was a number of companies. There were some pharmaceutical companies, et cetera. So there were companies that were badly hit. What people don't talk about, though, and this is kind of where I'm alluding to, is the companies that weren't hit and survived quite well during this pandemic. And there were a number of them actually physically located in Ukraine, had officers in Ukraine who would, in theory, have been exposed to that. And really what they did is all of the cybersecurity basics.

29:08
Speaker 1
They did their patch management rights, they had the latest version of patches, et cetera, and they weren't hit. And that's a critical part, because things like not pitcher and the WannaCry virus of a number of years ago were actually the consequence of cybersecurity. Tool sets that were lost by the US government. And they kind of got into what we call got into the wild and then started getting used by nation state actors. And then, unfortunately, the nation state actors then lose their tools and they're careless with them and then become in the hands of cybercriminals.

29:38
Speaker 1
And that's actually one of the reasons that I alluded to earlier as to why the threat landscape has got so much more severe, is you had tool sets that were being used by the cyber seven s of this world, which were well beyond the capabilities of your average cybercriminal. And now, unfortunately, they've carelessly kind of left those out for other people to use. So you've got these very sophisticated government level arsenals of weapons. And it's not just the Americans, it's everybody. They've all found ways to manage to stumble and lose their tool set. And the cybercriminals have now picked them up, which makes all of us much more vulnerable. But at the same time, the US government's done a huge job in terms of creating standards and things like that, which are bringing organizations into having much better security posture.

30:28
Speaker 1
So that's kind of where cybersecurity awareness month came. And I probably gave a little bit too much of a political tinge to it. I'm a little bit cynical about the US government and what they do, but they do a huge amount

of good as well in terms of this awareness and setting standards like the Nist standard for cybersecurity and things like that. So I guess the message that comes out of that, ultimately, is if you do all your basics right, you dramatically reduce the probability that you're going to get breached. And if you are breached, you find you're a lot more resilient. So your recovery, your ability to recover is significantly better.

31:04
Speaker 2
Yeah.

31:05
Speaker 3
Now I want to just touch on that, Brian, because you mentioned that we kind of lost all the stuff that we've done in the 90s. It's almost like the good stuff that we've done in the incorporating process networks, et cetera. With the advent of IoT devices, it's almost like we kind of lost those principles. If we think about the 1990s. We call it as the good old automation pyramid. They actually call it the Pera. The Pera is the prudence enterprise reference architecture guide where they develop different levels. So level zero is your equipment, level one is your control, level two is your SCaDA. Level three is then your more mes up until you get to level 100% relevant.

31:51
Speaker 2
Today it is got Iot on the.

31:53
Speaker 3
Side, but there was a very good way that we could segment the levels. And then either by implementing a very simple DMZ or a firewall between different levels, you could segregate the way of data flowing and possible keep the threat.

32:09
Speaker 2
Typically one direction only.

32:11
Speaker 3
Typical one direction. The problem was obviously, if you need to move from, let's say, your level three into the upper level, you needed Internet, et cetera. So that became a little bit crazy with getting all those trusts and policies in place. But what we're seeing now is we're not even going from level three to the Internet anymore. We're going from level zero to level one. We're bypassing all of those firewall kind of rules that we put in place with Lapera architecture. And while we're going straight into the cloud with this, obviously exposing risk. So I think what I'm trying to ask is, what is the new strategy? What is this basics that you need to go and look at and put in place?

32:51
Speaker 2
Yeah, we spoke about, tough question. We spoke about sort of aggressive patch management. We spoke about device and app controls and endpoint inventory and stuff like that. But if I'm a smallish to mid kind of manufacturer based somewhere in Joburg, I'm already dealing with the disruption to my operational resilience around, know, what are some of the key basic things? Perhaps not an easy one to answer. What are some of the key basics that I need to consider or have in place?

33:25
Speaker 1
Sure. So in the past, it was relatively easy to talk to that I guess. Now you got to think about your entire estate in terms of three zones. So in the old days, zone one was your perimeter, and you needed to protect your perimeter, and your perimeter was very easily defined, and you did that with a firewall. So it was perimeter and endpoint and then patch management, and you'd mostly covered 90% of your problem. There were some, obviously, there's always other elements, but in terms of the total number of threats that are hitting you, what's happened now is as people adopt cloud, they're starting to dissolve that perimeter.

33:58

Speaker 1
So you need to find ways to protect your perimeter in the cloud environment using something like in the email world, using something like mimecast, secure email gateway, in the web security world, using something like a web security gateway, all of those sorts of things. So it's critical to get that perimeter, because what you want to do is keep, absorb as many of the threats as you possibly can away from your network before they even get to you. The second zone you got to look at is inside your network. So those are your users, your insiders, those are your endpoints, those are your alerting systems that you need to put in place the sort of canaries in the coal mine. I'm not advocating any particular product set there, but there's a whole bunch of.

34:41
Speaker 3
Thanks for that.

34:44
Speaker 1
But there's a whole bunch of things that you can do in zone two, which is assume that you're going to stop most of the things in the perimeter, but also work on the principle that something will get through and work out what your insider threat looks like and what the assumption could look like. Yes, it's absolutely the assumption that something will get in and that something that could get in could actually be one of your own people. You get careless insiders, you get compromised insiders, and you get malicious insiders. So your own people can either be inadvertently doing something or doing something deliberate. And again, this is the whole Covid thing. Their spouse might have lost their job and they may not even want to do this, but they're desperate for extra money and somebody's paying them to actually create vulnerabilities.

35:21
Speaker 1
We see this with the mobile operators all the time in their call centers, where people are paying contact center workers to help them do sim swaps and things like that. So there's a lot of kind of move towards zero trust, only give people the access to what they absolutely need to do their jobs. The problem doesn't stop there. You then got to look outside your perimeter as well at your brand. So one of the things we see quite a little bit is what we call supply chain attacks, where people are either using you as the supplier to whoever your client is or attacking your supply chain. So whoever your suppliers are and say, you might have the most perfect security system in the world, but somebody else doesn't.

36:05
Speaker 1
We see that problem with the banks all the time, the supply chain management problem, we saw that recently with that big data breach with Experian. That was all bank data that they lost, but the banks were all fine.

36:15
Speaker 2
But Experian, very good point, especially in the manufacturing world, where there is such a very high reliance on multiple suppliers. You think about, for example, a beverage manufacturing company, there's almost nearly a seamless integration between systems, given, for example, the cans that have to be delivered and how those systems communicate and preempt the next delivery. That's actually a fascinating point, is that supply chain dependence between businesses.

36:44
Speaker 1
Yeah. So there's a couple of things that are very much in the infancy now, but I certainly expect to see them grow is this concept of threat intelligence sharing. In other words, if I see a threat on my system, I actually share it with everybody in my ecosystem, those kinds of things, and really starting to leverage what you already have in terms of the tools. The economy is not going to get better quickly and we're going to have to make do with what we have and not have to buy more and more expensive things necessarily, or when we do, we must obviously buy carefully. And so the key issue here is how do you make what you've already bought work better? And that's all about leveraging your ecosystem using APIs, using threat intelligence, getting things.

37:26
Speaker 1
If your firewall spots something, making sure your email gateway is aware of it, and vice versa. If there's a piece

of malware coming into one of your suppliers, make sure that your endpoint protection, your antivirus is aware of that same piece of malware. Those kinds of things are where we're going with this, but it's certainly not there yet and it's generally quite problematic. And I think the other issue is, which also goes to the just accept the fact that at some point you will be breached. There's that old statement, well, there's only two types of organizations and this is quite an old saw saying, those who've been breached and those who don't know they've been breached, but everybody's been breached. And all the statistics that you see kind of bear that out. In large part.

38:16
Speaker 1
It's just a question of the severity of the breach. And I think we're going to talking about breaches once the pop here, as we're supposed to call it, kicks into play in July next.

38:26
Speaker 2
Fully in effect yet?

38:28
Speaker 1
No. So we're in a grace period at the moment, but one of the things that you should be doing now is actually declaring a data breach if there is personally identifiable information that's been lost. And the definition of that is fairly broad. It could literally be something like somebody's phone number or home address or email that is still personally identical. So even if somebody breaches some very trivial system of yours and you lose a database of potential prospects or something, and it's just the name and email, that is still a notifiable breach that you have to tell the information regulator about. And I think we're going to see this absolute spike towards July and after July next year and everyone's going to go, what's happening? Why are we suddenly seeing this massive attack against South Africa? And the answer is, it's not new.

39:13
Speaker 1
We're just actually getting visibility now.

39:15
Speaker 2
Just actually getting the visibility. Yeah, I'm just cautious of time. Something I quickly want to ask you, Brian. I'm quite interested about it. So on the topic of remote working, so in our world, and I'm sure the disruption wasn't specific just to our industry, but all of a sudden, with working from home and Covid, all of a sudden a lot of these sort of manufacturing systems that we spoke about earlier that were not meant to be online suddenly with a number of sort of key people and resources working from home, all of a sudden these people now had to access these systems from home. They needed to in sort of ways, and routing and tunneling that they didn't have to ever do before in the past.

39:59
Speaker 2
So a key thing for the systems that we work with is the ability for people to actually connect to and operate and get reporting and viewing of these systems from home. Obviously, working from home, that does present not only all of a sudden a new way to sort of gain entry to the systems from home, but that presents a whole new different threat layer or area that we didn't see in the past.

40:29
Speaker 1
Absolutely. And I mean, that's probably a whole nother hour of conversation, but just at a high level, what we saw is organizations, first of all, scrambling to get everybody working from home quickly. And speed is always the enemy of security. So what we found is people having to turn off certain secure systems just so that they could help get everybody out there and working, not necessarily patching. Your visibility is a lot weaker, so you can't actually see if somebody's been compromised. If somebody has been compromised, your time to remediate is longer. But as you point out, it's a whole new set of vulnerabilities, unless you get people who's slightly paranoid, like me, and even as I say, no system is immune. But very few people have got network separation at home.

41:11

Speaker 1
Very few people have got sophisticated enterprise grade networking and security equipment at home. I mean, virtually nobody I know has their own firewall systems at home, other than the very simple network address translation type broadband routers and things. And we saw this happening as Covid struck. We saw a lot of these broadband routers and there were a number of them. So I'm not even going to call out the brand names suddenly got attacked en masse because people. And again, does your ISP upgrade your broadband router? Do you even know how to upgrade your broadband router? I guarantee that there's massive vulnerabilities all around the place, and I'm expecting to see this become a major point. And it already is. This home networking vulnerability combined with, as you say, this ability to connect you back to systems that should be very secure.

42:02
Speaker 1
We saw VPN systems being attacked quite dramatically and overwhelmed. They were designed for the few executives and road warriors to work remotely, not for the entire organization to work remotely. So we saw big challenges in terms of volume. And these haven't all gone away. I think they've largely kind of been settled, and I think a lot of companies are patting themselves on the back, but I think that's a little bit of false complacency to think that's now been resolved. And that's largely just because the threat actors don't need to. They work on the sort of path of least resistance. So you see them do that. If they spray and pray high volume, low sophistication attacks work, then they actually dial back on the ones that are harder to do because it's all about making money.

42:41
Speaker 1
But as we start closing up the loopholes, they find other ways to. And then all they do is move into other spaces which we just haven't had to defend against. And they find all kinds of loopholes, and then the whole cycle starts again. So I fully expect to see this being a huge area of focus over the next year or so.

42:57
Speaker 2
Yeah. And I suppose given the opportunistic nature of these cybercriminals or threat actors, they prey on a topic such as Covid-19 and that's also an entirely new area for them to exploit and make use of.

43:12
Speaker 1
Yeah. And they take advantage of the sort of psychological state that people are in. People are desperate for information. People are a bit depressed. People are in a funny state of mind when you're working from home. And they use those. It's called social engineering. And it's kind of just really just a fancy name for good old fashioned fraud. But it's very clever. It's like a con. In fact, a con is probably a better word. It's a cyber con, the old con man who kind of came along and snake oil salesman. They use all of those same techniques, but they do it in the digital environment and they're highly effective because people are people.

43:45
Speaker 2
Yeah, 100%. Cool. Fascinating stuff, chiefs. I think we're okay on time. We probably have to wrap it up, Brian. We can probably chat to you for hours and. Sounds like really scary stuff that's happening out there. And it's good to know that people like you are out there fighting the good fight. But maybe just as a recap, in terms of those zones that you mentioned, if you can just give us a recap of the important zones. I suppose it feels like I interrupted you on that?

44:14
Speaker 1
No, not at all. So zone one is really your perimeter. And bear in mind that your perimeter is now spread out into the cloud because we've got this cloud and digital adoption that just about everybody's gone to and make sure that you've got all those loopholes and security controls in place. Zone two is inside your network. Everything that involves being inside whatever that might be, people and systems. And then zone three is things like your brand and your overall ecosystem and your supply chain. It's everything else that's not either your perimeter or inside your perimeter. And if you can get those working effectively together, then you're going to go a long way to having a really good security posture and being more cyber resilient.

44:56

Speaker 2
Okay, fantastic.

44:58
Speaker 3
My closing remarks maybe just on this. Thanks a lot, Brian. You actually answered my question 100%.

45:06
Speaker 2
I feel a lot smarter now.

45:08
Speaker 3
I really want our listeners to go and.